UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PIERLUIGI CASTALDO individually and on behalf of all others similarly situated,	)	**Case No. 22-cv-8663**
Plaintiff,	)	**CLASS ACTION**
v.	)	
EMPRESS AMBULANCE SERVICES, LLC, d/b/a EMPRESS EMS,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Pierluigi Castaldo ("Plaintiff"), by and through his attorneys of record, upon personal knowledge as to his own acts and experiences, and upon information and belief as to all other matters, files this complaint against Defendant Empress Ambulance Services, Inc. d/b/a Empress EMS ("Defendant" or "EEMS") and alleges the following:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used to provide its services. This information includes, but is not limited to, personally identifiable information ("PII") and protected health information ("PHI"), including one or more of the

following: full name, Social Security number, health insurance information, and date(s) of service (collectively, "Sensitive Information") of approximately 318,558 individuals.[1]

2. Defendant EEMS has been operating for 37 years and has over 700 personnel.[2] EEMS claims it is "the premier provider of 9-1-1 emergency medical response for the cities of Yonkers, New Rochelle, Yorktown, Pelham, Poughkeepsie, Mount Vernon, White Plains, and the Bronx."[3] EEMS handles over fifty thousand transports a year.[4]

3. To obtain medical treatment, Plaintiff and other patients of Defendant entrust and provide to Defendant an extensive amount of highly sensitive and privileged PII. Defendant retains this information–even long after the treatment relationship ends. Defendants acknowledge the importance of the protected information.[5]

4. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and members of the proposed Class's PII, Defendant assumed legal and equitable duties to those individuals.

5. Plaintiff and members of the proposed Class are victims of Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Defendant's current and former patients.

6. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII and PHI. But Defendant betrayed that trust. Defendant failed to use reasonable, up-to-date security practices and protocols to prevent the Data Breach that occurred. Defendant further

[1] Exhibit 1, ("Website Notice of Privacy Incident"), available at https://empressems.com/notice-of-security-incident/ (last accessed Oct. 4, 2022). *See also* U.S. DHHS OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Oct. 4, 2022).

[2] *About*, EEMS (last accessed Oct. 4, 2022) available at https://empressems.com/about/

[3] *Services*, EEMS (last accessed Oct. 4, 2022) available at https://empressems.com/services/

[4] *Id.*

[5] Exhibit 2, ("Notice of Privacy Practices") available at https://empressems.com/wp-content/uploads/2022/07/empressprivacy.pdf (last accessed Oct. 4, 2022).

failed to provide a timely, adequate, and accurate notice to Plaintiff and members of the proposed Class.

7. On information and belief, Defendant first became aware of the Breach on July 14, 2022, after the unauthorized party downloaded Plaintiff's and Class Members' Sensitive Information from Defendant's systems.[6] According to Defendant, the Breach occurred from May 26, 2022, to July 14, 2022.[7] Defendant began notifying victims about the Data Breach on September 9, 2022.[8]

8. When Defendant announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's notice sent to impacted individuals fails to explain how many people were impacted, how the breach happened, and why the unauthorized party had unfettered access to Plaintiff's and the Class's Sensitive Information for almost 2 months before Defendant became aware of the Breach.

9. Plaintiff and members of the proposed Class are victims of Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Plaintiff and members of the Class.

10. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant did not maintain reasonable, up-to-date security practices and protocols to prevent the Data Breach that occurred. In fact, Defendant confirmed as much in its Breach Notice: "we strengthened the security of our systems and will continue enhancing our protocols to further safeguard the information in our care."[9]

---

[6] Ex. 1.

[7] *Id.*

[8] Exhibit 3, (Pierluigi Castaldo Notice Letter)

[9] *Id.*

11. Prior to notification of the breach, Plaintiff and members of the proposed Class had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will carry on for the duration of their lifetimes.

12. Defendant's failure to timely detect and adequately notify breach victims violates New York and Federal law and has made Plaintiff and members of the Class (defined *infra*) vulnerable to a present and continuing risk of fraud and identity theft.

13. For example, armed with Sensitive Information acquired in the Data Breach, data thieves are able to commit numerous crimes including opening new financial accounts in members of the proposed Class's names, using members of the proposed Class's names to obtain government benefits, filing fraudulent tax returns, obtaining driver's licenses in members of the proposed Class's names but with another person's photograph, giving false information to police during an arrest, taking out loans in members of the proposed Class's names, and using members of the proposed Class's names to obtain medical services. Accordingly, Plaintiff and members of the proposed Class must now and for the foreseeable future closely monitor their financial and other accounts to guard against identity theft and related harm.

14. As a result of Defendant's conduct, Plaintiff and the Class have and will be required to continue to undertake and incur out-of-pocket, expensive, and time-consuming efforts to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on medical portals, and requesting and maintaining accurate medical records outside of those kept by medical providers.

15. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used in its ordinary course of business.

16. Plaintiff and the members of the proposed Class therefore bring this lawsuit seeking remedies including damages, reimbursement of out-of-pocket-costs, and equitable and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and identity protection services funded by Defendant.

PARTIES

17. **Plaintiff Pierluigi Castaldo** is a resident and citizen of Yonkers, New York. Mr. Castaldo received a notice informing his that his Sensitive Information was compromised in the EEMS Data Breach.

18. **Defendant Empress Ambulance Services, Inc. d/b/a Empress EMS** is a corporation organized under the laws of New York and maintains its principal place of business at 722 Nepperhan Avenue, Yonkers, New York 10703.

19. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), and is a class action involving 100 or more class members. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over EEMS because EEMS is a corporation organized under the laws of New York and has its principal place of business at 722 Nepperhan Ave, Yonkers, New York, 10703.

22. Venue properly lies in this judicial district pursuant to 28 U.S.C. § 1391 because inter alia, the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this district; Defendant's principal place of business is in this district; Defendant transacts substantial business and has agents in this district; a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district; and because Plaintiff resides within this district.

FACTUAL BACKGROUND

A. Background

23. Defendant EEMS has been operating for 37 years and has over 700 personnel.[10] EEMS claims it is "the premier provider of 9-1-1 emergency medical response for the cities of Yonkers, New Rochelle, Yorktown, Pelham, Poughkeepsie, Mount Vernon, White Plains, and the Bronx." [11] EEMS handles over fifty thousand transports a year. [12]

24. To obtain healthcare and related services, patients, like Plaintiff and the Class, must provide Defendant with highly sensitive information, including PHI, PII, or both. Defendant compiles, stores, and maintains the highly sensitive PII and PHI. Defendant serves thousands of individuals per year indicating it has created and maintains a massive repository of Sensitive

[10] *See* Note 2, *supra.*

[11] *See* Note 3, *supra.*

[12] *Id.*

Information, acting as a particularly lucrative target for data thieves looking to obtain and misuse or sell patient data.[13]

25. Defendant posts a "Notice of Privacy Practices" on its website.[14] In it, Defendant claims that EEMS is committed to fully complying with HIPAA and with the protection of its patients' health information.[15] The Privacy Policy lists a number of permissible and expected uses of Plaintiff's and the Class's Sensitive Information, none of which is contemplated by the Data Breach here.

26. Plaintiff and the Class had a reasonable expectation that Defendant would protect the Sensitive Information provided to and created by it, especially because, given the publicity of other data breaches and the significant impact they had, Defendant knew or should have known that failing to adequately protect patient information could cause substantial harm. Moreover, through its Notice of Privacy Practices, Defendant acknowledged its obligation to reasonably safeguard sensitive information against security breaches and other types of theft and misuse.

27. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and the Class's Sensitive Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

---

[13] *Id.*

[14] Ex. 2.

[15] *Id.*

B. The Data Breach and Notice Letter

28. Beginning on May 26, 2022, to July 14, 2022, a malicious actor gained unauthorized access to Defendant's computer network and systems.[16] By doing so, the actor gained access to the sensitive personal, medical, and insurance information of Defendant's current and former patients. The malicious actors maintained unfettered access to Defendant's network and systems until Defendant remediated the breach on or around July 14, 2022. Upon information and belief, the actors copied and exfiltrated substantial amounts of Plaintiff's and the Class's PII and PHI.[17]

29. Defendant did not disclose the existence of the Data Breach to patients or the public until September 9, 2022. Defendant sent notices to the victims of the Data Breach warning them to take additional action to protect themselves from the potential risk of harm.[18] They also posted the notice of the Data Breach to the internet via a public statement.[19]

30. The Data Breach notices recommended Plaintiff and the Class take time-consuming steps to mitigate the risk of future fraud and identity theft.[20]

31. Given that Defendant was storing the PII and PHI of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. That obligation

[16] Ex. 1.
[17] *Id.*
[18] Ex. 3.
[19] *Id.*
[20] *Id.*

stems from the foreseeable risk of a Data Breach given that Defendant collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at different healthcare institutions and providers put Defendant on notice that the higher personal data it stored might be targeted by cybercriminals.

32. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry and the prevalence of health care data breaches, Defendant inexplicably failed to adopt sufficient data security processes, a fact highlighted in its notification to affected patients in which it revealed that only after the Data Breach, Defendant has taken steps to increase the security of its systems. EEMS stated, "we strengthened the security of our systems and will continue enhancing our protocols to further safeguard the information in our care."[21] Clearly, the Data Breach at issue here was the inevitable result of Defendant's inadequate approach and/or attention to data security protection of the Sensitive Information it collects, analyzes, and uses in its ordinary course of business.

33. The Data Breach itself, and the information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, the number of people impacted, and the sensitive nature of the impacted data collectively demonstrate Defendant failed to implement reasonable measures to prevent cyber-attacks and the exposure of the Sensitive Information they oversaw.

C. Exposure of Sensitive Information Creates a Substantial Risk of Harm

34. The personal, health, and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

[21] *Id.*

35. Defendant's failure to reasonably safeguard Plaintiff's and the Class's sensitive PHI and PII has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft.[22]

36. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[23] This is because stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

37. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

38. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help law enforcement stop fraudulent transactions and mitigate losses.

[22] The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority. 17 C.F.R. § 248.201 (2013).

[23] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

39. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[24]

40. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry unapproved activity;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function property;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[25]

41. The United States Government and the United States Cybersecurity & Infrastructure Security Agency recommend several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring

[24] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.

[25] *Start With Security, A Guide for Business*, FTC (last visited Jan. 18, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205.

firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

42. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[26] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendant failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

D. The Healthcare Industry is Particularly Susceptible to Cyber Attacks.

43. Data breaches have become alarmingly commonplace in the U.S. In 2021, data breaches increased by nearly 70% over the previous year, which is over 20% higher than the previous all-time high.[27]

44. The healthcare sector was the easiest "mark" among all major sectors last year, meaning it had the highest number of data compromises and categorically had some of the most widespread exposure per data breach.[28] According to the 2021 Healthcare Information and Management Systems Society Cybersecurity Survey, 67% of participating hospitals reported having a significant security incident within the last twelve months, with a majority of those being caused by "bad actors."[29]

---

[26] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[27] *2021 Annual Data Breach Year-End Review*, ITRC, (Jan. 2022), https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

[28] *Id.*

[29] *2021 HIMSS Cybersecurity Survey*, Healthcare Information and Management Systems Society, Inc., accessible at: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey (last accessed Mar. 16, 2022).

45. Healthcare providers and vendors that maintain health care provider data "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[30]

46. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[31] According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.[32] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[33]

47. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.[34]

---

[30] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospitaldata-from-email-spoofing-attacks.

[31] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), (last visited Jan. 11, 2021), https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

[32] *Id.*

[33] *Id.*

[34] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

48. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches, 472 of which had confirmed data disclosures in 2021.[35] For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.[36]

49. As a healthcare provider with hundreds of thousands of current and former patients, if not more, Defendant knew or should have known the importance of protecting the Sensitive Information entrusted to it. Defendant also knew or should have known of the foreseeable, and catastrophic consequences if its systems were breached. These consequences include substantial costs to Plaintiff and the Class because of the Data Breach. Despite this, Defendant failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

E. Plaintiff's and the Class's PHI and PII are Valuable.

50. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[37]

---

[35] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[36] *Five worthy reads: The never-ending love story between cyberattacks and healthcare*, ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

[37] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

51. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[38] For that reason, Cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as $300 per number.[39] Those numbers are often then used for fraudulent tax returns.[40]

52. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[41] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

53. Defendant's Data Breach exposed a variety of Sensitive Information, including Social Security numbers and PHI.

54. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit

[38] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[39] *Id.*

[40] *Id.*

[41] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

to apply for more credit in your name."[42] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

55. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

56. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation ("FBI") has found instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.[43]

57. Other reports found that PHI is ten times more valuable on the black market than credit card information.[44] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for $1-2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute.[45]

58. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

---

[42] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[43] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

[44] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[45] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

59. Because the Sensitive Information exposed in the Defendant's Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their Sensitive Information.

F. Defendant's Conduct Violates HIPAA

60. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[46]

61. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[47] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[48]

62. HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8) Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[49]

---

[46] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[47] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html.

[48] *Id.*

[49] *Id.*

63. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect. The Data Breach resulted from Defendant's failure to comply with several of these standards:

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits;

b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Violation of 45 C.F.R. § 164.308(a)(6)(ii): Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity;

e. Violation of 45 C.F.R. §164.306(a)(2): Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information;

f. Violation of 45 C.F.R. §164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

g. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by their workforce;

h. Violation of 45 C.F.R. §164.502, et seq: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

i. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

64. Despite Defendant's failure to reasonably protect Plaintiff's and the Class's Sensitive Information, they have not offered any compensation or adequate remedy considering

the significant and long-term risks Plaintiff and the Class face. Defendant has merely offered 12 months of identity protection services.[50]

PLAINTIFF'S EXPERIENCES

65. Pierluigi Castaldo is a resident and citizen of New York. He is a former patient of EEMS.

66. As a condition of receiving healthcare related services, EEMS required Pierluigi Castaldo to provide EEMS with his PII and PHI. Accordingly, Pierluigi Castaldo provided EEMS with his PII and PHI in order to purchase and receive healthcare services. Plaintiff believed his PII and PHI provided to EEMS for healthcare services would be protected by EEMS.

67. On or about September of 2022, Pierluigi Castaldo received notice from EEMS, which informed him of the Data Breach and that he faced a substantial and significant risk of his PII and PHI being misused.

68. Subsequent to and as a direct and proximate result of the Data Breach, Mr. Castaldo experienced a substantial number of spam emails, text, messages, and phone calls which Plaintiff believes is related to his private information being placed in the hands of an illicit actor. As a result, Mr. Castaldo had to spend considerable time and efforts to mitigate against any future identity theft and fraud. This included running an extensive background check on all of his Sensitive Information shortly after receiving the Notice Letter. Through running this background check, Mr. Castaldo was informed that his information is now on the dark web.

69. Plaintiff Castaldo is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff Castaldo stores any documents containing his sensitive information

[50] Ex. 3.

in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts. Finally, Plaintiff Castaldo has never previously had his identity stolen.

70. Plaintiff Castaldo suffered actual injury from having his sensitive information exposed and/or stolen as a result of the Data Breach including, but not limited to: (a) entrusting PII and PHI to EEMS that he would not have had EEMS disclosed it lacked data security practices adequate to safeguard its patients; (b) damages to and diminution in the value of his Sensitive Information–a form of intangible property that he entrusted to EEMS as a condition of receiving healthcare services; (c) loss of his privacy; (d) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and (e) time and expense of his mitigation efforts as a result of the data breach and subsequent exposure of his information on the dark web.

71. In addition, knowing that hackers accessed and/or stole his PII and PHI and that this information was published on the dark web, and will likely be used in the future for identity theft, fraud, and related purposes has caused Mr. Castaldo to experience feelings of anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

CLASS ALLEGATIONS

72. Pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff brings this action on behalf of himself and on behalf of all members of the proposed Classes (collectively, the "Class," "Classes," and "Class Members:) defined as:

> **Nationwide Class:** All individuals residing in the United States whose PII and/or PHI was stored or possessed by EEMS that was actually or potentially compromised during the Data Breach as referenced in the Notice of Data Privacy Incident provided by Defendant.[51]
>
> **New York Subclass**: All residents of the State of New York whose PII and/or PHI was stored or possessed by EEMS that was actually or potentially compromised during the Data Breach as referenced in the Notice of Data Privacy Incident provided by Defendant.[52]

73. The following people are excluded from the Classes: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parents have a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

74. Plaintiff and members of the Classes satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Federal Rule of Civil Procedure 23.

[51] Ex. 1.

[52] *Id.*

75. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The exact number of members of the Classes are unknown but, upon information and belief, they are estimated to number in the tens or hundreds of thousands at this time, and individual joinder in this case is impracticable.[53] Members of the Classes can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

76. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of the claims of other members of the Classes in that Plaintiff, and the members of the Classes sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and members of the Classes sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

77. **Adequacy, Fed. R. Civ. P. 23(a)(4)**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Classes. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Classes, and Defendant has no defenses unique to Plaintiff.

78. **Commonality and Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3)**: There are many questions of law and fact common to the claims of Plaintiff and the Classes, and those

[53] EEMS reported the Breach as impacting approximately 318,558 to the U.S. DHHS Office for Civil Rights, U.S. DHHS OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Oct. 4, 2022).

questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

a. Whether Defendant violated the laws asserted herein;

b. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff's and members of the Classes' PII and PHI;

c. Whether Defendant breached the duty to use reasonable care to safeguard members of the Classes' PII and PHI;

d. Whether Defendant knew or should have known about the inadequacies of their data security policies and system and the dangers associated with storing sensitive PII and PHI;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and members of the Classes' PII and PHI from unauthorized release and disclosure;

f. Whether Defendant breached its contractual promises to safeguard Plaintiffs' and members of the Class's PII and PHI;

g. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff's and members of the Classes' PII and PHI from unauthorized release and disclosure;

h. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

i. Whether Defendant's delay in informing Plaintiff and members of the Classes of the Data Breach was unreasonable;

j. Whether Defendant's method of informing Plaintiff and other members of the Classes of the Data Breach was unreasonable;

k. Whether Defendant is liable for negligence or gross negligence;

l. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PII and PHI violated applicable state laws;

m. Whether Plaintiff and members of the Classes were injured as a proximate cause or result of the Data Breach;

n. What the proper measure of damages is; and

o. Whether Plaintiff and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

79. **Superiority, Fed. R. Civ. P. 23(b)(3):** This cause is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

80. A class action is therefore superior to induvial litigation because:

a. The amount of damages available to an individual Plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS

COUNT I
Negligence
(On behalf of Plaintiff and the Nationwide Class)

81. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

82. Defendant collected, created, and maintained Plaintiff's and the Class's Sensitive Information for the purpose of providing medical or related services to Plaintiff and the Class.

83. Plaintiff and the Class are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures. The nature of Defendant's business requires patients to disclose Sensitive Information to receive adequate care, including, but not limited to, medical histories, dates of birth, addresses, phone numbers, and medical insurance information. Thus, for Defendant to provide its services, it must use, handle, gather, and store the Sensitive Information of Plaintiff and the Class

and, additionally, solicit and create records containing Plaintiff's and the Class's Sensitive Information.

84. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that, given its repository of a host of Sensitive Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

85. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

86. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the Class's PHI and PII was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

87. Defendant also had a duty to timely and adequately disclose to Plaintiff and the Class that their Sensitive Information had been or was reasonably believed to have been compromised. Timely and adequate disclosure is necessary so that, among other things, Plaintiff and the Class may take appropriate measures to monitor their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions, including those recommended by Defendant.

88. Additionally, HIPAA creates industry standards for maintaining the privacy of health-related data. Defendant knew or should have known it had a legal obligation to secure and protect Plaintiff's and the Class's Sensitive Information and that failing to do so is a serious violation of HIPAA.

89. Defendant also should have known that, given the Sensitive Information it held, Plaintiff and the Class would be harmed should it suffer a Data Breach. Defendant knew or should have known that its systems and technologies for processing and securing Plaintiff's and the Class's PHI and PII had security vulnerabilities susceptible to cyber-attacks.

90. Despite that knowledge, Defendant failed to implement reasonable data security measures which allowed cybercriminals to successfully breach Defendant's network and data environments, reside there undetected for a significant period of time, and access or steal a host of personal and healthcare information on thousands of Defendant's patients.

91. Defendant, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

92. Defendant breached its duty to Plaintiff and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiff's and the Class's PHI and PII, and failing to recognize the Data Breach in a timely manner. Defendant further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiff's and the Class's PHI and PII.

93. But for Defendant's wrongful and negligent breach of its duties, their Sensitive Information would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

94. As a result of Defendant's negligence, Plaintiff and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

95. As a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class suffered and continue to suffer injuries and are entitled to and demand actual, consequential, and nominal damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
15 U.S.C. § 45
(On behalf of Plaintiff and the Nationwide Class)

96. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

97. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

98. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PHI and PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

99. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

100. Plaintiff and the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

101. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures, caused the same harm suffered by Plaintiff and the proposed Class.

102. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries as described herein and are entitled to damages in an amount to be proven at trial.

COUNT III
Negligence *Per Se*
HIPAA, 45 C.F.R. § 160.102
(On behalf of Plaintiff and the Nationwide Class)

103. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

104. Defendant required Plaintiff and the Class to provide nonpublic Sensitive Information to obtain medical services. During the provision of those services, Defendant created and stored even more PHI.

105. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

106. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information."

107. Per 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation specifications" apply to covered entities, such as Defendant. HIPAA standards are mandatory.

108. HIPAA requires Defendant to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably anticipated threats or hazards to the security or integrity" of the Sensitive Information. 45 C.F.R. § 164.306.

109. Defendant violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

110. Defendant violated HIPAA by failing to use reasonable measures to protect the PII and PHI of Plaintiff and Class. Defendant's conduct was especially unreasonable given the nature of the Sensitive Information and the number of patients it serves, some of which are minors or patients who live below the federal poverty level, who may not have the means to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

111. Defendant's violation of HIPAA constitutes negligence *per se*. Plaintiff and the Class are within the group of individuals HIPAA was designed to protect and the harm to these individuals is a result of the Data Breach.

112. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries as described herein and are entitled to damages in an amount to be proven at trial.

COUNT IV
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Nationwide Class)

113. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

114. Plaintiff and members of the Class incorporate the above allegations as fully set forth herein.

115. Defendant owed a fiduciary duty to Plaintiff and the Class to protect their private and sensitive PHI and PII and keep them apprised of when that information becomes exposed or compromised in an accurate manner.

116. Defendant breached that fiduciary duty by, inter alia, failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and members of the Class. This failure resulted in the Data Breach that ultimately came to pass.

117. Defendant further breached its fiduciary duty by failing to dispose of PHI and PII that was no longer required to render care, which unnecessarily exposed additional patients—including Plaintiff—to the Data Breach, and by failing to accurately inform Plaintiff and the Class of the Data Breach which materially impaired their mitigation efforts.

118. As a direct and proximate cause of Defendant's breaches of its fiduciary duty, Plaintiff and members of the Class have suffered and will suffer injury, including but not limited to: (a) the compromise, publication, theft, and /or unauthorized use of their PII and PHI; (b) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences

of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) the continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect PII and PHI in its possession; and (e) current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

119. Plaintiff, on behalf of himself and the Class, seeks actual, consequential, and nominal damages and injunctive relief for breach of fiduciary duty.

COUNT V
Breach of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

120. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

121. In connection with receiving healthcare services, Plaintiff and members of the Class entered into implied contracts with Defendants.

122. Pursuant to these implied contracts, Plaintiff and members of the Class paid money to Defendant and provided Defendant with their PH/PHI. In exchange, Defendant agreed to, among other things, and Plaintiff understood that Defendant would: (1) provide health care to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PH/PHI; and (3) protect Plaintiff's and Class members PH/PHI in compliance with federal and state laws and regulations and industry standards.

123. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members and Defendant. Defendant recognized the importance of data security

and the privacy of its patients' PII/PHI in its Notice of Privacy Practices. Had Plaintiff and Class members known that Defendant would not adequately protect its patients' and former patients' PII/PHI, they would not have received health care services from Defendant.

124. Moreover, express and implied in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their PII or PHI. [54]

125. Plaintiff and the members of the Class would not have entrusted their PII and PHI to Defendant in the absence of such agreement with Defendant.

126. Defendant materially breached the contract(s) it entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them adequately of the Data Breach that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff' and members of the Class's PII and PHI;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

127. Plaintiff and all other Class members were damaged by Defendant's breach of implied contracts because: (i) they paid-directly or through their insurers-for data security

[54] Ex. 2.

protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical identity theft-risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

128. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

129. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

130. Plaintiff and members of the Class have sustained damages as a result of Defendant's breaches of its agreement.

131. Plaintiff, on behalf of himself and members of the Class, seeks nominal damages and compensatory damages for breach of implied contract, which include, but are not limited to, the lost benefit of their bargain with Defendant and the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

132. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

133. Plaintiff and members of the Class conferred a monetary benefit upon Defendant in the form of monies paid for healthcare services.

134. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff' and members of the Class's PII and PHI, as this was used to facilitate its provision of healthcare services.

135. As a result of Defendant's conduct, Plaintiff and members of the Class suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and members of the Class paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

136. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that Plaintiff and members of the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

137. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VII
Violation of the New York Deceptive Acts and Practices Act
N.Y. Gen. Bus. Law § 349 ("GBL")
(On behalf of Plaintiff and the New York Subclass)

138. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

139. Plaintiff Castaldo and New York Subclass members are "persons" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(h).

140. EEMS is a "person, firm, corporation or association or agent or employee thereof" within the meaning of the GBL. N.Y. Gen. Bus. Law § 349(b).

141. Under GBL section 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce" are unlawful.

142. EEMS violated the GBL through its promise to protect and subsequent failure to adequately safeguard and maintain Plaintiff and Class members' PII/PHI. EEMS failed to notify Plaintiff and other class members that, contrary to its representations about valuing data security and privacy, it does not maintain adequate controls to protect PII/PHI. It omitted all of this information from Plaintiff and class members.

143. As a result of EEMS's above-described conduct, Plaintiff and the New York Subclass have suffered damages from the disclosure of their information to unauthorized individuals.

144. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of EEMS's violations of the GBL. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the

effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

145. Plaintiff Castaldo, individually and on behalf of the New York Subclass, requests that this Court enter such orders or judgments as may be necessary to enjoin EEMS from continuing its unfair and deceptive practices.

146. Under the GBL, Plaintiff and New York Subclass members are entitled to recover their actual damages or $50, whichever is greater. Additionally, because Defendant acted willfully or knowingly, Plaintiff Castaldo and the New York Subclass members are entitled to recover three times their actual damages. Plaintiff Castaldo also is entitled to reasonable attorneys' fees.

PRAYER FOR RELIEF

147. WHEREFORE, Plaintiff respectfully prays for judgment in his favor as follows:

a. Certification of the Class pursuant to the provisions of Fed. R. Civ. Pro. 23 and an order that notice be provided to all Class Members;

b. Designation of Plaintiff as representative of the Class and the undersigned counsel, as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. Pre-judgment interest at the maximum amount allowed by law;

f. Post-judgment interest at the maximum rate allowed by law;

g. An award of costs and attorneys' fees; and

h. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

148. Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

Dated: October 12, 2022

REESE LLP

/s/ Michael R. Reese
Michael R. Reese
100 West 93rd Street, 16th Floor
New York, New York 10025
Tel: (212) 643-0500
mreese@reesellp.com

Brian C. Gudmundson*
Jason P. Johnston*
Michael J. Laird*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Christopher D. Jennings*
Nathan I. Reiter III*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, Arkansas 72201
Tel: (501) 372-1300
chris@yourattorney.com
nathan@yourattorney.com

*To be admitted *pro hac vice*

Counsel for Plaintiff and the Proposed Class